Notice of Allowability	Application No.	Applicant(s)	
	09/668,026	JENNINGS, WILLIAM T.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *16 February 2007*.

2. ☒ The allowed claim(s) is/are *1-6,8-24,26-33,35 and 36*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS **THREE-MONTH PERIOD IS NOT EXTENDABLE**.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date MAILED w/ NOA
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Bradley Bowling (Reg. No. 52,641) on 16 April 2007.

The application has been amended as follows:

Claim 6: (Currently Amended) A method for storing and withdrawing decryption keys from a key escrow database, comprising:

generating at a computer, in accordance with a selected encryption function, a set of N cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of N cryptogram/decryption key pairs and the corresponding token to a receiver, the transmission sent over a communication path coupling the receiver and the computer;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key;

generating a cryptogram utilizing the corresponding decryption key and comprising the selected token and randomization information;

recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; ~~and~~

inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database[[.]];

randomly selecting at the receiver one or more additional cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the corresponding token of the additionally selected encryption/decryption key pairs to identify a corresponding decryption key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding decryption key and comprising the selected additional token(s) and randomization information; and

mixing the token information from one selected key pair with the response cryptogram from a different selected key pair along with randomization information to diffuse response structure prior to generating another response cryptogram.

Claim 7: (Cancelled)

Claim 8: (Currently Amended) The method for storing and withdrawing decryption keys from a key escrow database as in Claim [[7]] 6, further comprising:

decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information.

Claim 33: (Currently Amended) A method for storing and withdrawing decryption keys from a key escrow database, comprising:

generating at a computer, in accordance with a selected encryption function, a set of N cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of N cryptogram/decryption key pairs and the corresponding token to a receiver, the transmission sent over a communication path coupling the receiver and the computer;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key;

generating a cryptogram utilizing the corresponding decryption key and comprising the selected token and randomization information;

recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token;

recording in an escrow database the generated cryptogram based on the randomly selected cryptogram/decryption key pair;

retrieving from the key escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token, and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; ~~and~~

inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database[[.]];

randomly selecting at the receiver one or more additional N cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the corresponding token of the additionally selected encryption/decryption key pairs to identify a corresponding decryption key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding decryption key and comprising the selected additional token(s) and randomization information;

mixing the token information from one selected key pair with the response cryptogram from a different selected key pair along with randomization information to diffuse response structure prior to generating an additional response cryptogram; and

recording in an escrow database the generated additional response cryptogram.

Claim 34: (cancelled)

DETAILED ACTION

3. Claims 1-6, 8-24, 26-33, 35, and 36 have been present examination.

4. Claim 25 has been cancelled as per Applicant's request.

5. Claims 7 and 34 have been cancelled as per Examiner's Amendment above.

6. Claims 1-6, 8-24, 26-33, 35, and 36 are allowable.

Response to Arguments

7. Applicant's arguments, see page 3, filed 16 February 2007, with respect to the prior art rejection of 1-24 and 26-36 have been fully considered and are persuasive. The rejection of claims 1-6, 8-24, 26-33, 35, and 36 has been withdrawn.

Allowable Subject Matter

8. The following is an examiner's statement of reasons for allowance:

As per claims 1, 6, 14, 28, and 33, the prior art has shown that it is well known in the art for key escrow systems similar to that disclosed by the Applicant in independent claims 1, 6, 14, 28, and 33. The prior art has also shown that padding is a common technique used for many reasons, for example padding is used to make encryption easier when using DES.

There are no teachings in the prior art of a key escrow system adding randomization information to the selected data to diffuse response structure. Since no teachings or motivation can be found a key escrow system adding randomization information to the selected data to diffuse response structure, claims 1-6, 8-24, 26-33, 35, and 36 are therefore novel and non-obvious.

9. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100